

OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 20

November 27, 2012


SUBJECT: INTERNET USAGE GUIDELINES - REVISED

PURPOSE: The Internet Usage Guidelines are revised to require Department employees to obtain commanding officer's approval prior to deviating from the Department's internet guidelines.

PROCEDURE: Attached is the revised Manual Section 3/788.40, *Internet Usage Guidelines*, with revisions indicated in italics.

AMENDMENTS: This Order amends Section 3/788.40 of the Department Manual.

AUDIT RESPONSIBILITY: The Commanding Officer, Internal Audits and Inspections Division, will review this directive and determine whether an audit or inspection will be conducted in accordance with Department Manual Section 0/080.30.

A handwritten signature in black ink, appearing to be 'C. Beck'.

CHARLIE BECK
Chief of Police

Attachment

DISTRIBUTION "D"

**DEPARTMENT MANUAL
VOLUME III
Revised by Special Order No. 20, 2012**

788.40 INTERNET USAGE GUIDELINES. The use of the Internet or e-mail on a Department computer shall be restricted to "official Department business." Personal use of *the Department computer* or time spent *on it* for personal gain is prohibited. Violation of any of these guidelines may be considered misconduct and may result in disciplinary action.

These guidelines are applicable to all City- or Department-owned or controlled computers (LAN, Personal Computers and Laptops) and telephone lines. This includes access to computers at sites and facilities that are owned, leased, rented, or utilized by Department employees. Department employees utilizing the Internet or e-mail shall cooperate with any investigation regarding the use of computer equipment.

Department employees shall not:

- Gain access to or transmit California Law Enforcement Telecommunications System (CLETS) information through the Internet, including secondary dissemination of Criminal History Record information through a communications media such as Internet e-mail facilities and remote access file transfer;
- Conduct an unauthorized attempt to enter into any other computer, known as hacking, which is a violation of the Federal Electronic Communications Privacy Act (FECPA) 18 United States Code 2510;
- Copy or transfer electronic files without permission from the copyright owner;
- Send, post, or provide access to any confidential Department materials or information;
- Send private or confidential e-mail as delineated in Manual Section 4/105.15;
- Transmit chain letters;
- Send threatening, slanderous, offensive, racially and/or sexually harassing messages; and,
- Represent oneself as someone else, real or fictional, or send messages anonymously.

Note: Use of the Internet for certain investigations may require a deviation from the Internet guidelines. This could include the use of offensive language, impersonation, or use of an alias, and the accessing or downloading of offensive or explicit material. *Department personnel must submit an Employee's Report, Form 15.07.00, and obtain approval from his/her commanding officer prior to engaging in such conduct. The Employee's Report must be filed in the employee's divisional package.* When conducting a Department authorized investigation that requires these tactics for investigative purposes, they are not considered misconduct.

In addition to these general guidelines, employees utilizing the Internet are advised that the Department has the right to access all e-mail files created, received, or stored on Department systems, and such files can be accessed without prior notification.